Influence of User Perception, Security Needs, and Social Factors on Device Pairing Method Choices

Iulia Ion
Institute for Pervasive Computing
ETH Zurich

1 Introduction

With the increasing proliferation of mobile devices, the need to spontaneously connect two devices over a wireless link (to exchange business cards and appointments, send files to Bluetooth-enabled printers, and to make electronic payments in busses, train stations, and coffee shops) has become prominent. To authenticate spontaneous wireless device communication, several secure device pairing protocols have been proposed in the literature that allow device authentication in the absence of a centralized security infrastructure. With no wires to verify actual connection, users cannot be sure what device they connected their wireless link to. The basic solution is the use of an "out-of-band" channel, i.e., a secondary information channel, to verify the authenticity of the primary wireless link. An example is the popular Bluetooth pairing method of displaying a 6-8 digit number on one device, and having the user enter it on the other [1]. Here, the user's eyes and fingers act as a secondary communication channel between the two devices. Consequently, the usability of such methods is of crucial importance, as complex mechanisms might raise the probability of human error, might prompt users to choose a lower security level, or lead them to abandon security altogether. We conducted an explorative study with 25 participants to determine the usability of proposed pairing methods *in specific situations*, and to elicit the needs and the underlying mental models of users with respect to their security considerations in device pairing scenarios.

2 Related Work

The last few years saw a number of studies that evaluated many of the hitherto proposed device pairing methods. Kumar et al. [6] tested 14 methods, resulting in almost 50 individual test cases that each participant had to perform. Participants were mostly "technology-savvy" university students, with 70% male participants. The role of social context and user security perception were not explored. In Kobsa et al. [5], participants were told to imagine that they had just bought a new phone and when they return home they want to pair it to the old one. No insight into *why* users thought that a particular method would be more secure than another is given. Kainda et al. [4] placed a stronger emphasis on the trade-off between usability of a method and its susceptibility to security failures.

3 Approach and Uniqueness

Our work differs from previous studies in three important points: (1) we explored user preferences not in terms of pure pairing speed but by investigating particular situations and their corresponding social factors; (2) we reduced mental load by testing only four representative pairing methods that a wide range of channels (visual, audio, tactile), and degrees of user involvement (from completely passive to very active); (3) we recruited participants with diverse, non-technical backgrounds, and aimed for a more balanced gender composition.

We explored what security levels users keep in given situations, and how much time and effort they are willing to spend. We therefore designed the four selected methods – *Select the device* with PIN entry [1], *Take a picture* [7], *Listen up* [3], and *Push the button* [8] – to run under three incremental security levels. To avoid bias, in the beginning we did not reveal that our study focused on security. Participants learned the four methods in their non-secure variant, in a pseudo-random order, and were then asked which method they would choose in three given real-world situations: (1) *printing a confidential financial report* in an airport lounge; (2) *making a mobile payment* in a duty-free shop, under stress; (3) *exchanging electronic business cards* with a newly-met CEO. Semi-structured interviews explored different factors influencing user choice. Next, a security briefing was given and the different security levels for each method were introduced. Participants were then asked to redo the tasks, this time choosing the preferred method and security level. Explorative interviews followed each task. Sessions lasted approximatively 70 minutes.

4 Results and Conclusions

Users varied both the security level and the method used depending on a wide range of factors: data sensitivity, the place and social setting, the time pressure, the person operating the other device, and perceived security threat. For example, when dealing with sensitive data, control and feedback is needed and, when handling less sensitive data or under time pressure, automatic methods are preferred. Furthermore, social factors influence greatly method requirements. If interacting with a friend, the method can be playful, but with a newly met person in a business environment professionally is required. Similarly, in the office, at home, in a public place, or in a meeting, different methods and security levels are desired.

Our results show that users do worry about security, but not in terms of malicious attackers or data encryption. A method is perceived as secure if it reassures users through double confirmation and control that they connected to the intended device. For some users, perceived security was more important than the predefined security levels. Understanding what makes people perceive a method as secure is of crucial importance in designing systems. Furthermore, we detected several mismatches between users' mental models and systems design, of which security designers should be aware. Finally, we proved that no single method is adequate for all situations. Designers should account for social factors and provide appropriate methods for different situations; users are likely to bypass security before breaking social norms.

Acknowledgements

We would like to thank Lorrie Cranor for guidance in planning the pilot studies, and Jonathan McCune for discussion on methods and security levels design.

References

[1] Bluetooth SIG. Bluetooth Special Interest Group. Simple Pairing Whitepaper (Revision V10r00), 2006.

[2] L. F. Cranor, editor. *Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS 2009, Mountain View, California, USA, July 15-17, 2009*, ACM International Conference Proceeding Series. ACM, 2009.

[3] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. Loud and clear: Human-verifiable authentication based on audio. In *ICDCS '06: Proceedings of the 26th IEEE International Conference on Distributed Computing Systems*, page 10, Washington, DC, USA, 2006. IEEE Computer Society.

[4] R. Kainda, I. Flechais, and A. W. Roscoe. Usability and security of out-of-band channels in secure device pairing protocols. In Cranor [2].

[5] A. Kobsa, R. Sonawalla, G. Tsudik, E. Uzun, and Y. W. 0005. Serial hook-ups: a comparative usability study of secure device pairing methods. In Cranor [2].

[6] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun. Caveat emptor: A comparative study of secure device pairing methods. In *PerCom*, pages 1–10. IEEE Computer Society, 2009.

[7] J. M. McCune, A. Perrig, and M. K. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *Proc. IEEE Symp. on Security and Privacy*, pages 110–124. IEEE CS Press, 2005.

[8] C. Soriente, G. Tsudik, and E. Uzun. BEDA: Button-enabled device pairing. In *Proc. IWSSI 2007*, pages 443–449, September 2007.